IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

BRANDON FRANKLIN, MARTA RAYKHSHTAT, CASEY CREANEY, and GARRETT STANWICK Individually and on behalf of the classes described below, Plaintiffs, vs. UBER TECHNOLOGIES, INC. Defendant.	)	Case No. 17-cv-8510 **PLAINTIFFS DEMAND TRIAL BY JURY**

CLASS ACTION COMPLAINT

Plaintiffs, BRANDON FRANKLIN, MARTA RAYKHSHTAT, CASEY CREANEY, and GARRETT STANWICK, individually and on behalf of the class members described below, by and through their undersigned attorneys, complain against Defendant UBER TECHNOLOGIES, INC. as follows:

I. INTRODUCTION

1. Plaintiffs bring this class action against UBER TECHNOLOGIES, INC. ("Uber") for its failure to secure and safeguard its customers' and drivers' PII ("PII").

2. In October 2016 Uber suffered a data breach and paid a bribe to keep the breach quiet rather than notify its customers of the breach.

3. Uber put profits over people with its attempt to sweep the data breach under the rug.

4. Plaintiffs and Class Members are Uber customers who booked rides, and were drivers in October 2016.

II. JURISDICTION AND VENUE

5. Jurisdiction is proper in this Court pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d).

6. Aggregate claims of individual Class Members exceed $5,000,000, exclusive of interest and costs.

7. At least one Class Member is a citizen of another state. 28 U.S.C. § 1332(d)(1)(D).

8. Venue lies properly within the Northern District of Illinois pursuant to 28 U.S.C. § 1391(b) because Defendant does business in this district and all of the events giving rise to Plaintiffs claims took place in this district.

III. THE PARTIES

9. Plaintiff, Brandon Franklin, is a retail consumer residing in Chicago, Illinois.

10. Plaintiff, Marta Raykhshtat, is a retail consumer residing in Barrington, Illinois.

11. Plaintiff, Casey Creaney, is a retail consumer residing in Encinitas, California.

12. Plaintiff, Garrett Stanwick, is a retail consumer residing in San Diego, California

13. Defendant Uber Technologies, Inc. is a corporation headquartered in San Francisco, California organized and existing under Delaware Law and operated its business in Chicago, Illinois.

14. The Uber provides car service worldwide via an on-demand dispatch system that enables users to hail a car service driver using a mobile phone through the application, and which enables transportation providers to accept and fulfill such on-demand requests for transportation services by users seeking transportation services through the use of a driver's application.

IV. FACTS COMMON TO ALL COUNTS

15. On November 21, 2017, Uber's CEO, Dara Khosrowshahi disclosed: "I recently learned that in late 2016 we became aware that two individuals outside the company had inappropriately accessed user data stored on a third-party cloud-based service that we use." (Statement from Khosrowshahi attached hereto as Exhibit "A" and incorporated herein).

16. In late 2016, Uber became aware that two individuals outside the company had inappropriately accessed user data stored on a third-party cloud-based service that we use.

17. The individuals were able to download files containing a significant amount of customer and driver information including: the names and driver's license numbers of around 600,000 drivers in the United States and personal information of 57 million Uber users around the world including names, email addresses and mobile phone numbers.

18. Uber claims to have taken immediate steps to secure the data and shut down further unauthorized access by the individuals at the time of the incident but never told its customers or drivers of the breach until over a year later.

19. Uber paid a $100,000 ransom to the criminals who stole the PII rather than come clean to its drivers and consumers.

20. Paying a ransom to the criminals who stole the data only compounds the problem and encourages future attacks.

21. FBI Cyber Division Assistant Director James Trainor said "Paying a ransom doesn't guarantee an organization that it will get its data back—we've seen cases where organizations never got a decryption key after having paid the ransom. Paying a ransom not only emboldens current cyber criminals to target more organizations, it also offers an incentive for other

criminals to get involved in this type of illegal activity. And finally, by paying a ransom, an organization might inadvertently be funding other illicit activity associated with criminals."[1]

22. Uber failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the data breach.

23. Plaintiffs and Class Members' PII is private and sensitive in nature and was inadequately protected by Uber.

24. Uber did not obtain Plaintiffs' and Class Members' consent to disclose their PII, except to certain persons not relevant to this action, as required by applicable law and industry standards.

25. It is incorrect to assume that reimbursing a consumer for a financial loss due to fraud makes that individual whole again.

26. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights.

27. Class Members are incurring and will continue to incur such damages in addition to any fraudulent credit and debit card charges incurred by them and the resulting loss of use of their credit and access to funds, whether or not such charges are ultimately reimbursed by the credit card companies. As Chief Judge Lasnik observed when sentencing a thief of PII, "identity theft can create huge emotional problems for people. We often think of bank fraud as just against a bank or just money, but it damages real people." Chief Judge Lasnik also noted that the damage of identity theft isn't just financial, "it causes rifts between husbands and wives, it causes divorces."[2]

[1] https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise/incidents-of-ransomware-on-the-rise

[2] Press Release, United States Attorney's Office, Western District of Washington, Member of ID Theft Ring That Preyed on Starbucks' Employees Sentenced to Prison (June 2, 2006), available at http://www.usdoj.gov/usao/waw/press/2006/jun/nguyen.htm (last visited Apr. 28, 2009).

28. The data breach was a direct and proximate result of Uber's failure to properly safeguard and protect Plaintiffs' and Class Members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Uber's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class Members' PII to protect against reasonably foreseeable threats to the security or integrity of such information.

29. As a direct and proximate result of Uber's wrongful action and inaction and the resulting data breach, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time and effort to mitigate the actual and potential impact of the subject data breach on their lives by, among other things, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring their credit reports and accounts for unauthorized activity.

30. Plaintiffs have suffered sufficiently concrete injuries for the purposes of Article III standing.

31. The "risk of real harm" is sufficient in this circumstance to constitute injury in fact.[3] The nature of a data breach, makes it so that the threatened injury is "certainly impending" as opposed to merely speculative.[4] The reason for that, is that the very nature of a data breach stems from individuals attempting to use the stolen information – this "intangible injury" has already occurred.[5] The harm in a data breach occurs to every affected individual that has had their

[3] *Lujan v. Defs. Of Wildlife*, 504 U.S. 555, 578 (1992).
[4] *Clapper v. Amnesty International USA*, 133 S. Ct. 1138, 1147-48 (2013)
[5] *See Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1549 (2016).

information acquired without their consent. Whether anticipated conduct or an anticipated injury is likely to happen after a breach is beside the point.

32. At a Federal Trade Commission ("FTC") public workshop in 2001, then Commissioner Orson Swindle described the value of a consumer's personal information as follows: "The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information."[6]

33. Though Commissioner's Swindle's remarks are more than a decade old, they are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 billion per year online advertising industry in the United States.[7]

34. Companies, in fact, also recognize PII as an extremely valuable commodity akin to a form of personal property. For example, Symantec Corporation's Norton brand has created a software application that values a person's identity on the black market.[8]

35. The FTC has also recognized that consumer data is a new – and valuable – form of currency. In a recent FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point by observing: "Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be

[6] The Information Marketplace: Merging and Exchanging Consumer Data, http://www.ftc.gov/bcp/workshops/infomktplace/transcript.htm (last visited Dec. 20, 2013)
[7] See Web's Hot New Commodity: Privacy, http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html (last visited Dec. 20, 2013).
[8] Risk Assessment Tool, Norton 2010, www.everyclickmatters.com/victim/assessment-tool.html. See also T. Soma, ET AL, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 RICH. J.L. & TECH. 11, at *3-4 (2009).

commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit."[9]

36. Recognizing the high value that consumers place on their PII, many companies now offer consumers an opportunity to sell this information to advertisers and other third parties. The idea is to give consumers more power and control over the type of information that they share – and who ultimately receives that information. And by making the transaction transparent, consumers will make a profit from the surrender of their PII.[10]

37. Consumers place a high value not only on their PII, but also on the privacy of that data. Researchers have already begun to shed light on how much consumers value their data privacy – and the amount is considerable. Indeed, studies confirm that "when [retailers'] privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[11]

38. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

39. Because Plaintiff and the Class were denied privacy protections that they paid for and were entitled to receive, Plaintiff and the Class incurred actual monetary damages in that they overpaid for the services provided by Uber.

---

[9] Statement of FTC Commissioner Pamela Jones Harbour (Remarks Before FTC Exploring Privacy Roundtable), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf (last visited Dec. 20, 2013).
[10] You Want My Personal Data? Reward Me for It, http://www.nytimes.com/2010/07/18/business/18unboxed.html (last visited Dec. 20, 2013).
[11] Hann et al., The Value of Online Information Privacy: An Empirical Investigation (Mar. 2003) at 2, available at http://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (emphasis added) (last visited Dec. 20, 2013); Tsai, Cranor, Acquisti, and Egelman, The Effect of Online Privacy Information on Purchasing Behavior, 22(2) Information Systems Research 254, 254 (June 2011)

40. Plaintiff and the Class suffered additional damages arising from the costs associated with identity theft and the increased risk of identity theft caused by Uber's wrongful conduct.

41. Plaintiff and the Class suffered additional damages based on the opportunity cost and value of time that Plaintiff and the Class have been forced to expend to monitor their financial and bank accounts as a result of the data breach.

42. Uber's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiffs and Class Members' PII, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. Theft of their PII;

b. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

c. The untimely and inadequate notification of the data breach;

d. The improper disclosure of their PII;

e. Loss of privacy;

f. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the data breach;

g. Ascertainable losses in the form of deprivation of the value of their PII, for which there is a well-established national and international market; and

h. Overpayments to Uber for booking rides and fees to drivers during the subject data breach in that a portion of the price paid for such booking by Plaintiffs and Class Members to Uber was for the costs of reasonable and adequate safeguards and security measures that would protect customers' PII, which Uber and its

affiliates did not implement and, as a result, Plaintiffs and Class Members did not receive what they paid for and were overcharged by Uber.

1) BRANDON FRANKLIN

43. Brandon Franklin was a driver engaged with Uber from April 13, 2015 to November 13, 2017.

44. Brandon Franklin, beginning in approximately 2015 and at all times relevant to this complaint, was an Uber consumer paying for Uber rides throughout Cook County.

45. Brandon Franklin's PII was stolen from Uber.

2) Marta Raykhshtat

46. Marta Raykhshtat, beginning in approximately 2015 and at all times relevant to this complaint, was an Uber consumer paying for Uber rides throughout Cook County.

47. Since learning of the data breach as alleged herein Marta Raykhshtat has paid for identity theft protection services.

48. Marta Raykhshtat's PII was stolen from Uber.

3) Casey Creaney

49. Casey Creaney, beginning in approximately 2015 and at all times relevant to this complaint, was an Uber consumer paying for Uber rides throughout Southern California.

50. Casey Creaney's PII was stolen from Uber.

4) Garret Stanwick

51. Garret Stanwick, beginning in approximately 2015 and at all times relevant to this complaint, was an Uber consumer paying for Uber rides throughout Southern California.

52. Garret Stanwick's PII was stolen from Uber.

V. CLASS ALLEGATIONS

53. Plaintiffs bring this action pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of themselves and the following proposed classes:

National Consumer Class
All persons residing in the United States whose PII was disclosed in the data breach in 2016.

National Driver Class
All Uber drivers residing in the United States whose PII was disclosed in the data breach in 2016.

Illinois Consumer Subclass
All members of the Nationwide Consumer Class who are residents of Illinois who purchased Uber services in Illinois.

Illinois Driver Subclass
All members of the Nationwide Driver Class who are residents of Illinois who utilized Uber services in Illinois.

California Consumer Subclass
All members of the Nationwide Consumer Class who are residents of California who purchased Uber services in California.

54. Upon information and belief, the proposed Class comprises millions of consumers throughout the nation, and is so numerous that joinder of all members of the Class is impracticable. While the exact number of Class Members is presently unknown and can only be ascertained through discovery, Plaintiffs believe that there are millions of Class Members.

55. There are numerous questions of law or fact common to the members of the Class which predominate over any questions affecting only individual members and which make class certification appropriate in this case, including:

a. Whether Uber owed a duty of care to Plaintiffs and Class Members with respect to the security of their personal information;

b. Whether Uber took reasonable steps and measures to safeguard Plaintiffs' and Class Members' personal information;

c. Whether Uber violated California's Unfair Competition Law by failing to implement reasonable security procedures and practices;

d. Whether Uber violated common and statutory law by failing to promptly notify Class Members their PII had been compromised;

e. Whether Uber has an implied contractual obligation to use reasonable security measures;

f. Whether Uber has complied with any implied contractual obligation to use reasonable security measures;

g. Whether Uber acts and omissions described herein give rise to a claim of negligence;

h. Whether Uber knew or should have known of the security breach prior to its November 2017 disclosure;

i. Whether Uber had a duty to promptly notify Plaintiffs and Class Members that their personal information was, or potentially could be, compromised;

j. What security measures, if any, must be implemented by Uber to comply with its implied contractual obligations;

k. What the nature of the relief should be, including equitable relief, to which Plaintiffs and the Class Members are entitled; and

l. Whether Plaintiffs and the Class are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

56. Unless an injunction is issued, Defendant will continue to commit the violations alleged, and the members of the proposed Class and the general public will continue to be misled and harmed.

57. This class action satisfies the criteria set forth in Fed. R. Civ. P. 23(a) and 23(b)(3) in that Plaintiffs are members of the Class; Plaintiffs will fairly and adequately protect the interests of the members of the Class; Plaintiffs' interests are coincident with and not antagonistic to those of the Class; Plaintiffs have retained attorneys experienced in class and complex litigation; and Plaintiffs have, through their counsel, access to adequate financial resources to assure that the interests of the Class are adequately protected

58. A class action is superior to other available methods for the fair and efficient adjudication of this controversy for at least the following reasons:

a. It is economically impractical for most members of the Class to prosecute separate, individual actions;

b. After the liability of Defendant has been adjudicated, the individual and aggregate claims of all members of the Class can be determined readily by the Court; and

c. Litigation of separate actions by individual Class members would create the risk of inconsistent or varying adjudications with respect to the individual Class members that would substantially impair or impede the ability of other Class members to protect their interests.

59. Class certification is also appropriate because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate declaratory and/or injunctive relief with respect to the claims of Plaintiff and the Class Members.

VI. CLAIMS

COUNT I
(NEGLIGENCE)
On Behalf of Nationwide Class and Each Subclass

60. Plaintiffs, Brandon Franklin, Marta Raykhshtat, Casey Creaney, and Garrett Stanwick, on behalf of themselves and the Nationwide Class and each Subclass, reallege and incorporate by reference herein the allegations contained in Paragraphs 1 through 59 as Paragraph 60 of Count I of the Complaint as if fully set forth herein.

61. Defendant actively solicited Plaintiffs and the other Class Members to use their PII in transactions with Uber.

62. When Plaintiffs and the other Class Members gave their PII to Defendants to facilitate and close transactions, they did so with the mutual understanding that Defendants had reasonable security measures in place and Defendant would take reasonable steps to protect and safeguard the PII of Plaintiffs and the other Class Members.

63. Consumer Plaintiffs and the other Class members also gave their PII to Defendants on the premise that Defendant was in a superior position to protect against the harms attendant to unauthorized access, theft and misuse of that information.

64. Upon accepting Plaintiffs' and Class Members' PII in their respective point-of-sale systems, Uber undertook and owed a duty to Plaintiffs and Class Members to exercise reasonable care to secure and safeguard that information from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties, and to utilize commercially reasonable methods to do so.

65. This duty included, among other things, designing, maintaining, and testing Uber's security systems to ensure that Plaintiffs' and the Class Members' PII was adequately secured and protected.

66. Uber further had a duty to implement processes that would detect a breach of its security system in a timely manner.

67. Uber had a duty to timely disclose to Plaintiffs and Class Members that their PII had been or was reasonably believed to have been compromised. Timely disclosure was appropriate so that, among other things, Plaintiffs and Class Members could take appropriate measures to avoid use of bank funds, and monitor their account information and credit reports for fraudulent activity.

68. Uber breached its duty to discover and to notify Plaintiffs and Class Members of the unauthorized access by failing to discover the security breach within reasonable time and by failing to notify Plaintiffs and Class Members of the breach until November of 2017.

69. To date, Uber has not provided sufficient information to Plaintiffs and Class Members regarding the extent and scope of the unauthorized access and continues to breach its disclosure obligations to Plaintiffs and the Class.

70. Uber also breached its duty to Plaintiffs and Class Members to adequately protect and safeguard this information by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PII. Furthering its negligent practices, Uber failed to provide adequate supervision and oversight of the PII with which it is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a third party to gather Plaintiffs' and Class Members' PII, misuse the PII, and intentionally disclose it to others without consent.

71. Through Uber's acts and omissions described in this Complaint, including Uber's failure to provide adequate security and its failure to protect Plaintiffs' and Class Members' PII from being foreseeably captured, accessed, disseminated, stolen, and misused, Uber unlawfully

breached its duty to use reasonable care to adequately protect and secure Plaintiffs and Class Members' PII during time it was within Uber's control.

72. Further, through its failure to timely discover and provide clear notification of the data breach to consumers and driver, Uber prevented Plaintiffs and Class Members from taking meaningful, proactive steps to secure their PII.

73. Upon information and belief, Uber improperly and inadequately safeguarded the PII of Plaintiffs and Class Members in deviation from standard industry rules, regulations, and practices at the time of the data breach.

74. Uber's failure to take proper security measures to protect Plaintiffs and Class Members' sensitive PII as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Plaintiffs and Class Members' PII.

75. Uber's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the PII; failing to conduct adequate regular security audits; failing to provide adequate and appropriate supervision of persons having access to Plaintiffs' and Class Members' PII.

76. Neither Plaintiffs nor the other Class Members contributed to the data breach and subsequent misuse of their PII as described in this Complaint. As a direct and proximate result of Uber's negligence, Plaintiffs and Class Members sustained actual losses and damages as described in detail above.

COUNT II
(BREACH OF IMPLIED CONTRACT)
On Behalf of Nationwide Class and Each Subclass

77. Plaintiffs, Brandon Franklin, Marta Raykhshtat, Casey Creaney, and Garrett Stanwick, on behalf of themselves and the Nationwide Class and each Subclass, reallege and incorporate by reference herein the allegations contained in Paragraphs 1 through 59 as Paragraph 77 of Count II of the Complaint as if fully set forth herein.

78. Uber's system solicited and invited Plaintiffs and the members of the Class to book rides, and for drivers to drive customers.

79. Plaintiffs and Class Members accepted Uber's offers and booked rides through Uber.

80. When Plaintiffs and Class Members booked rides through Uber, they provided their PII. In so doing, Plaintiffs and Class Members entered into implied contracts with Uber to which Uber agreed to safeguard and protect such information and to timely and accurately notify Plaintiffs and Class Members if their data had been breached and compromised.

81. Each booking made with Uber's system by Plaintiffs and Class Members was made pursuant to the mutually agreed-upon implied contract with Uber and the drivers using their system under which Uber agreed to safeguard and protect Plaintiffs' and Class Members' PII and to timely and accurately notify them if such information was compromised or stolen.

82. Plaintiffs and Class Members would not have provided and entrusted their PII to Uber in the absence of the implied contract between them and Uber.

83. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Uber.

84. Uber breached the implied contracts it made with Plaintiffs and Class Members by failing to safeguard and protect the PII of Plaintiffs and Class Members and by failing to provide timely and accurate notice to them that their PII was compromised as a result of the data breach.

85. As a direct and proximate result of Uber's breaches of the implied contracts between Uber and Plaintiffs and Class Members, Plaintiffs and Members sustained actual losses and damages as described in detail above.

COUNT III
(UNJUST ENRICHMENT)
On Behalf of Nationwide Class and Each Subclass

86. Plaintiffs, Brandon Franklin, Marta Raykhshtat, Casey Creaney, and Garrett Stanwick, on behalf of themselves and the Nationwide Class and each Subclass, reallege and incorporate by reference herein the allegations contained in Paragraphs 1 through 59 as Paragraph 86 of Count III of the Complaint as if fully set forth herein.

87. Uber has received and retained a benefit from Plaintiffs and the Class Members and inequity has resulted.

88. Uber has benefitted from providing a service without paying for adequate security and Plaintiffs and Class Members have overpaid for a service that is not in fact secure.

89. Thus, Class Members conferred a benefit on Uber by paying full price for a service that had already been exposed by criminals.

90. It is inequitable for Uber to retain these benefits.

91. Plaintiffs were not aware of the true facts about the data breach until over a year later, and did not benefit from Uber's conduct.

92. Uber knowingly accepted the benefits of its unjust conduct.

93. As a result of Uber's conduct, the amount of its unjust enrichment should be disgorged, in an amount according to proof.

COUNT IV
(VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW, CAL. BUS. & PROF. CODE § 17200, ET SEQ.)
On Behalf of Nationwide Class and California Subclass

94. Plaintiffs, Brandon Franklin, Marta Raykhshtat, Casey Creaney, and Garrett Stanwick, on behalf of themselves and the Nationwide Class and the California Subclass, reallege and incorporate by reference herein the allegations contained in Paragraphs 1 through 59 as Paragraph 94 of Count IV of the Complaint as if fully set forth herein.

95. Uber is a California Corporation with its principal office in San Francisco, California.

96. California Business & Professions Code § 17200 prohibits acts of "unfair competition," including any "unlawful, unfair or fraudulent business act or practice" and "unfair, deceptive, untrue or misleading advertising." Uber engaged in conduct that violated each of this statute's three prongs.

97. Uber committed an unlawful business act or practice in violation of Cal. Bus. & Prof. Code § 17200, *et seq*., when it failed to disclose to consumers that their PII was in the hands of criminals.

98. Uber committed unfair and fraudulent business acts and practices in violation of Cal. Bus. & Prof. Code § 17200, *et seq*., when it affirmatively misrepresented, actively concealed, and/or failed to disclose the true the data breach detailed herein.

99. Uber committed unfair and fraudulent business acts and practices in violation of Cal. Bus. & Prof. Code § 17200, *et seq*., when in failed to secure customer data and instead pay a $100,000 ransom to criminals who stole customer and driver PII.

100. Uber disseminated unfair, deceptive, untrue and/or misleading statements regarding the security of Uber.

101. In addition, Uber engaged in unlawful acts and practices with respect to its services by failing to discover and then disclose the data breach to Plaintiffs and Class Members in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82. To date, Uber has still not provided such sufficient information to Plaintiffs and the Class Members.

102. Uber knew or should have known that its system had been breached and data security practices were inadequate to safeguard Class Members' PII and that the risk of a data breach or theft was highly likely. Uber's actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Class Members.

103. Uber's unfair or deceptive acts or practices occurred repeatedly in the course of Uber's trade or business in California, and were capable of deceiving a substantial portion of the purchasing public nationwide.

104. As a direct and proximate result of Uber's unfair and deceptive practices, Plaintiffs and Class Members have suffered and will continue to suffer actual damages.

105. As a result of its unfair and deceptive conduct, Uber has been unjustly enriched and should be required to make restitution to Plaintiffs and Class Members pursuant to Cal. Bus. & Prof. Code §§ 17203 and 17204.

COUNT V
(VIOLATION OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT, 815 ILCS 501/1 et seq)
On Behalf Illinios Subclasses

106. Plaintiffs, Brandon Franklin and Marta Raykhshtat on behalf of themselves and the Illinois Subclasses, reallege and incorporate by reference herein the allegations contained in Paragraphs 1 through 59 as Paragraph 106 of Count V of the Complaint as if fully set forth herein.

107. The Illinois Consumer Fraud and Deceptive Business Practices Act ("ICFA"), 815 ILCS §§ 505/1, *et seq*., provides protection to consumers by mandating fair competition in commercial markets for goods and services.

108. The ICFA prohibits any deceptive, unlawful, unfair, or fraudulent business acts or practices including using deception, fraud, false pretenses, false promises, false advertising, misrepresentation, or the concealment, suppression, or omission of any material fact, or the use or employment of any practice described in Section 2 of the "Uniform Deceptive Trade Practices Act". 815 ILCS § 505/2.

109. Plaintiffs and the other members of the Illinois Subclasses were deceived by Uber's failure to properly implement adequate, commercially reasonable security measures to protect their private financial information while utilizing Uber.

110. Uber intended for Plaintiffs and the other members of the Illinois Subclasses to rely on Uber to protect the information furnished, in such manner that the transactions would be protected, secure, and not susceptible to access from unauthorized third parties.

111. Uber instead handled Plaintiffs' and the other Class Members' PII in such manner that it was compromised.

112. Uber failed to follow industry best practices concerning data theft or was negligent in preventing such data theft from occurring.

113. It was foreseeable that Uber's willful indifference or negligent course of conduct in handling its customers' personal information would put that information at risk of compromise by data thieves.

114. Uber benefited from mishandling its customers' personal information because, by Uber saved on the cost of those security measures.

115. Uber's fraudulent and deceptive acts and omissions were intended to induce Plaintiff's and the other Class Members' reliance on Uber's deception that their financial information was secure and protected when using debit and credit cards utilize Uber.

116. Uber violated 815 ILCS 505/2 by failing to properly implement adequate, commercially reasonable security measures to protect Plaintiffs and the other Illinois Subclass Members' private financial information.

117. Uber's acts or practice of failing to employ reasonable and appropriate security measures to protect consumers' PII constitute violations of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

118. Uber's conduct constitutes unfair acts or practices as defined in that statute because Uber caused substantial injury to Class Members that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers.

119. Uber also violated 815 ILCS 505/2 by failing to immediately notify affected customers of the nature and extent of the data breach pursuant to the Illinois Personal Information Protection Act, 815 ILCS 530/1, et seq., which provides:

> Sec. 10. Notice of Breach. (a) Any data collector that owns or licenses personal information concerning an Illinois resident **shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. The disclosure notification shall be made in the most expedient time possible and without unreasonable delay**, consistent with any measures necessary to determine the scope of the breach and

> restore the reasonable integrity, security, and confidentiality of the data system. (emphasis added)

120. 815 ILCS 530/20 provides that a violation of 815 ILCS 530/10 "constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act."

121. Plaintiffs and the other Illinois Subclass Members have suffered injury in fact and actual damages including lost money and property as a result of Uber's violations of 815 ILCS 505/2.

122. Plaintiff and the other Class members' injuries were proximately caused by Uber's fraudulent and deceptive behavior, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is appropriate

123. By this conduct, Uber violated the substantive consumer protection and unfair deceptive trade practices acts or statutes of the Consumer Fraud States, whose laws do not materially differ from that of Illinois, or conflict with each other for purposes of this action.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of members of the Nationwide Class and Classes, respectfully request that the Court enter judgment in their favor and against Defendant, as follows:

A. Certification of the proposed Class, including appointment of Plaintiffs' counsel as Class Counsel;

B. An order temporarily and permanently enjoining Uber from continuing the unlawful, deceptive, fraudulent, and unfair business practices alleged in this Complaint;

C. Costs, restitution, damages, including punitive damages, penalties, and disgorgement in an amount to be determined at trial;

D. An order requiring Uber to pay both pre- and post-judgment interest on any amounts awarded;

E. An award of costs and attorneys' fees; and

F. Such other or further relief as may be appropriate.

Respectfully submitted,
BRANDON FRANKLIN, MARTA RAYKHSHTAT, CASEY CREANEY, and GARRETT STANWICK
Plaintiffs,

By: */s/Alexander N. Loftus*
Attorney for Plaintiffs

Andrew Stoltmann, Esq.
Alexander N. Loftus, Esq.
Joe Wojciechowski, Esq.
Deanna LaPage, Esq.
STOLTMANN LAW OFFICES, P.C.
10 S. LaSalle Street, Suite 3500
Chicago, Illinois 60603
PH: (312) 332-4200
andrew@stoltlaw.com
alex@stoltlaw.com
joe@stoltlaw.com
deanna@stoltlaw.com

Dated: November 22, 2017